(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 709 903**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **93 10781**

(51) Int Cl⁶ : H 04 L 9/30, H 04 M 3/22, H 04 Q 3/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 10.09.93.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 17.03.95 Bulletin 95/11.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *Société dite: THOMSON-CSF (Société anonyme)* — FR.

(72) **Inventeur(s)** : Damour Christian.

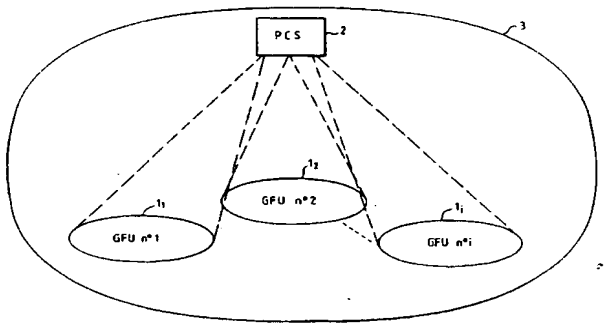
(73) **Titulaire(s)** :

(74) **Mandataire** : Leroux Jean-Philippe Thomson-CSF.

(54) Procédé et dispositif de sécurisation de communications utilisant un réseau numérique à intégration de services.

(57) Le procédé selon l'invention consiste à définir un nouveau complément de service intitulé groupe fermé d'usagers sécurisé (1_1 à 1_i) accessible aux usagers par abonnement, dans l'environnement d'un point de commande des services (2) du RNIS (3). Pour établir au moins une communication sécurisée entre au moins deux correspondants abonnés d'un même service, quelque soit le service, la sécurisation étant transparente vis-à-vis de chacun des correspondants pour le service demandé, le procédé consiste à reconnaître par un commutateur d'accès au service du RNIS (3), le complément de service groupe fermé d'usagers sécurisé, à aiguiller la signalisation usager à usager vers le point de commande des services (2) du RNIS (3), à authentifier les correspondants en instance de communication, et à contrôler le droit d'accès des correspondants par une lecture d'une base de données contenant la liste des abonnés au complément de service groupe fermé d'usagers sécurisé.

Les applications vont aux communications intra et interbancaires, aux communications à caractère sensible dans le cadre institutionnel, aux communications d'entreprise etc.



FR 2 709 903 - A1

Procédé et dispositif de sécurisation de communications utilisant un réseau numérique à intégration de services.

La présente invention concerne un procédé et un dispositif de sécurisation de communications utilisant un réseau numérique à intégration de services dénommé ci-après RNIS.

Le domaine d'application de la présente invention est très vaste car il couvre tous les services de télécommunications mis à la disposition des usagers d'un réseau de type RNIS. Il couvre notamment les communications intra et interbancaires, les communications à caractère sensible dans le cadre institutionnel, les communications d'entreprises etc...

Un RNIS comporte un ensemble de possibilités fonctionnelles qui permettent d'offrir, aux usagers pouvant être répartis sur différents sites d'activité et qui lui sont raccordés, une série de services de télécommunications tels que des services support, téléservices et compléments de service. Les services support et téléservices sont offerts seuls en tant que services de base alors que les compléments de service accompagnent obligatoirement l'un des deux précédents.

Les services support correspondent à la fourniture des possibilités du réseau relatives aux couches inférieures du réseau c'est-à-dire aux couches 1 à 3 du modèle de référence pour l'interconnexion des systèmes ouverts connu également sous l'abréviation anglo-saxonne OSI "Open System Interconnection". Ce modèle a été initialement élaboré par l'ISO, abréviation anglo-saxonne pour "International Organization for Standardization". Les services support sont offerts à l'interface entre un terminal et le réseau et se rapportent au transfert d'informations. Les téléservices sont des services offerts à un usager en aval du terminal et comprennent des fonctions relatives à l'ensemble des couches 1 à 7 correspondant aux couches inférieures, 1 à 3, et couches supérieures, 4 à 7, du modèle OSI. Les compléments de services correspondent à des possibilités optionnelles s'appliquant aux services support et aux téléservices. Ces possibilités sont additives ou modificatrices de celles des services de base et concernent principalement les facultés et le confort de mise en oeuvre des services. Les RNIS qui utilisent la signalisation CCITT n° 7, abréviation pour Comité Consultatif International Télégraphique et Téléphonique, assurent la fourniture des services supports et téléservices

pour permettre de satisfaire des besoins variés pour des usagers qui pourront bénéficier d'une même gamme étendue de services ainsi regroupés sur un même accès comme par exemple le télex, la télécopie, le vidéotex, le visiophone et la téléphonie etc... Cette signalisation utilise un principe de signalisation par canal sémaphore qui repose sur le transfert d'informations de commande par une liaison de transmission de données commune à plusieurs circuits. La signalisation par canal sémaphore se situe au confluent des évolutions de la commutation fondée sur la commande à programme enregistré et de la transmission de données dont elle applique les principes selon le modèle OSI. Le système associé à cette signalisation est constitué de deux grands ensembles de fonction : le sous-système de transport de messages SSTM et les sous-systèmes utilisateurs SSU.

Le raccordement des usagers au réseau public RNIS recouvre l'ensemble des moyens mis en oeuvre depuis le terminal jusqu'au commutateur public d'usagers. Les spécifications des interfaces usagers/réseaux font appel aux notions de canal, structure d'interfaces et capacité d'accès, sur la base d'un nombre limité de type de canaux et de structure d'interfaces. Ces interfaces usagers/réseaux sont au nombre de deux : la première interface à débit de base supporte deux canaux B et un canal D, et une deuxième interface à débit primaire supporte trente canaux B et un canal D.

Le canal B est un canal à 64 Kbits/s commuté en mode circuit ou en mode paquet qui peut être utilisé pour transporter tous types d'informations. Le canal D est un canal à 16 ou 64 Kbits/s fonctionnant en mode message apte à transporter la signalisation et des services en mode paquet. Ces interfaces sont polyvalentes dans le sens où chacune d'entre elles est apte, dans la limite de son débit propre, à fournir l'ensemble des services offerts par le réseau. Les protocoles d'accès du RNIS étendent le concept de signalisation par canal sémaphore jusqu'aux équipements terminaux des installations d'usagers ou installations terminales d'usagers, ITU. Le canal D de l'accès usager/réseau transporte la signalisation relative aux canaux B du même accès. La signalisation mise en oeuvre entre l'usager et le réseau permet l'établissement des connexions nécessaires au transfert des informations entre usagers ainsi que la réalisation des compléments de services.

Parmi ces compléments de service la signalisation d'usager à usager SUU offre un moyen supplémentaire de transfert d'informations entre usagers. Un complément de service particulier, appelé groupe fermé d'usagers, GFU, permet la constitution, à partir du réseau public, de réseaux privés virtuels cloisonnés les uns par rapport aux autres, auxquels ne peuvent accéder que les abonnés au GFU qui leur est attribué. Ce complément de service est apporté par le service TRANSGROUPE, marque déposée par France Télécom, et exploite les capacités de réseau intelligent supportées par l'architecture CAS, abréviation pour Commutateur d'Accès au Service, et PCS abréviation et marque déposée par France Télécom signifiant Point de Commande des Services.

Les autres compléments de service concernent les services du type "identification des appels".

L'appelant dans le cas du RNIS peut refuser de s'identifier par exemple par la non communication de son numéro d'appelant au destinataire ce qui fait l'objet d'un complément de service dédié. Ce complément de service a été imposé par la CNIL, abréviation pour Commission Nationale Informatique et Liberté, et se trouve rendu nécessaire dans le cas d'un usager du RNIS utilisant le service téléphonique tout en étant sur la liste rouge. Celui-ci souscrit dans ce cas un abonnement pour le complément de service intitulé "secret de l'identité du demandeur". L'usager demandé est alors informé de l'application "secret de l'identité du demandeur". Dans un premier temps néanmoins une solution provisoire doit être mise en place consistant à réserver l'identification de l'appelant à la transmission de données. Par ailleurs il est vraisemblable qu'une décision administrative doit s'appliquer à l'interdiction de connaître l'identité du demandeur pour les fournisseurs de certains services, par exemple dans le cas d'une commande par correspondance. Cependant une possibilité demeure pour l'usager d'identifier l'origine d'un appel, en s'abonnant au complément de service intitulé "identification d'appels malveillants". Ce complément de service permet à l'usager demandé de déclencher le mécanisme d'identification du demandeur RNIS, au cours ou à la fin de cette communication, dans un délai maximum de 30 secondes. Cette information d'identification soumise à la discrétion de l'exploitant doit faciliter la découverte de l'origine d'appels malveillants ou gênants et n'est disponible

pour l'exploitant qu'après la fin de la communication. Elle est constituée des éléments suivants :

- identification complète du demandeur sous la forme de son numéro RNIS,
- date et heure de la demande d'identification, et
- numérotation composée par le demandeur de la communication.

Toutefois la communication de ces informations d'identification à l'usager plaignant dépend d'une décision judiciaire coûteuse en démarches et en temps.

Le but de l'invention est de pallier les inconvénients précités.

A cet effet, l'invention a pour objet un procédé de sécurisation d'un réseau numérique à intégration de services, ou RNIS, du type mettant en oeuvre un ensemble de téléservices offerts aux usagers du réseau, avec des options appelées compléments de service, caractérisé en ce qu'il consiste pour définir un nouveau complément de service intitulé groupe fermé d'usagers sécurisé accessible aux usagers par abonnement, dans l'environnement d'un point de commande des services du RNIS, à reconnaître par un commutateur d'accès au service du RNIS, le complément de service groupe fermé d'usagers sécurisé, à aiguiller la signalisation d'usager à usager vers le point de commande des services du RNIS, à authentifier les correspondants en instance de communication et, à contrôler les droits d'accès des correspondants par une lecture d'une base de données contenant la liste des abonnés au complément de service groupement fermé d'usagers sécurisé, pour permettre d'établir au moins une communication sécurisée entre au moins deux correspondants abonnés d'un même service, quel que soit le service, la sécurisation étant transparente vis-à-vis de chacun des correspondants pour le service demandé

L'avantage du procédé selon l'invention est qu'il permet d'assurer des communications sécurisées entre deux utilisateurs abonnés à un même service RNIS, quel que soit celui-ci Le service et le nouveau complément de service "groupe fermé d'usagers sécurisé", ou GFU sécurisé, sont gérés par le PCS du RNIS de telle sorte que la sécurisation est effectuée en toute transparence vis-à-vis du service, c'est-à-dire sans incidence sur le service proposé par le RNIS aux usagers abonnés.

La présente invention exploite les capacités de réseaux intelligents apportées par une architecture similaire à celle d'un commutateur d'accès au service, CAS, et d'un point de commande des services PCS qui sont des appellations relatives au RNIS français connu sous le nom de marque commerciale NUMERIS de France Télécom.

Dans le but de simplification concernant la terminologie utilisée dans cette description, les termes CAS et PCS sont conservés pour les fonctions similaires utilisées par l'invention.

D'autres avantages et caractéristiques de l'invention apparaîtront plus clairement en regard des dessins annexés qui représentent :

la figure 1, un schéma simplifié représentant des groupes fermés d'usager gérés par le PCS,

la figure 2, une représentation simplifiée du principe utilisé par le procédé selon l'invention,

la figure 3, un schéma de principe de la fonction de distribution et de gestion de clés utilisée par le procédé selon l'invention,

la figure 4, un premier mode de réalisation d'un dispositif pour la mise en oeuvre du procédé selon l'invention

la figure 5, une représentation d'une structure en couches suivant le modèle OSI d'une communication sécurisée entre deux usagers d'un même GFU selon l'invention, et

la figure 6, un deuxième mode de réalisation d'un dispositif selon l'invention.

La présente invention respecte la numérisation et la signalisation hors bande qui sont les deux principes sur lesquels repose l'intégration des services au sein d'un RNIS.

Dans un premier temps, la sécurisation se limite aux accès de base c'est-à-dire à la gestion séparée des deux canaux B et du canal D en mode paquet ou circuit et se réserve la possibilité d'étendre le service à valeur ajoutée de communication sécurisée via RNIS aux accès primaires c'est-à-dire aux trente canaux B et au canal D, ainsi qu'à tout autre type d'accès en nombre, en type de canaux et en débit.

Comme décrit précédemment l'invention utilise l'environnement de développement du PCS.

La figure 1 illustre un schéma simplifié symbolisant la gestion de réseaux privés virtuels utilisant les compléments de services "groupement fermé d'usagers" GFU respectivement GFU n° 1, 1_1, GFU n° 2, 1_2, ..., GFU n° i, 1_i, via le PCS 2 du RNIS 3. Chaque groupement fermé d'usagers, GFU n° 1 à N° i, 1_1 à 1_i, est composé d'un ensemble d'installations terminales d'usagers ITU entre lesquelles des communications sécurisées sont possibles. Les communications d'un GFU déterminées sont cloisonnées par rapport aux autres GFU.

La figure 2 illustre de façon simplifiée le principe utilisé par le procédé selon l'invention lors de l'établissement d'une communication entre un usager appelant A et un usager appelé B. Le RNIS 4 se caractérise par une signalisation hors bande 5, régie par la norme C.C.I.T.T. n° 7, acheminée par le réseau sémaphore qui est indépendant du réseau de transmission de données. Par conséquent, dès lors que la signalisation d'usager à usager SUU de demande d'établissement a abouti respectivement à l'installation terminale de l'usager appelant ITU A, 6, et de l'usager appelé ITU B, 7, l'usager appelant A peut prendre possession du circuit physique. Le RNIS 4 comporte un commutateur d'accès au service CAS 8 placé sous le contrôle du point de commande des services PCS 9 capable de gérer un demi-appel amont avec l'appelant A et un demi-appel aval avec l'appelé B auxquels sont associées des informations de signalisation distinctes et repérées par une étiquette qui les associe aux demi-appels. Ce n'est que sur ordre du PCS 9 que le CAS 8 met effectivement en relation les deux correspondants A et B.

En cas d'accord du PCS 9 sur la demande d'établissement de liaison suite à la consultation de sa base de données BD 10, celui-ci opère une conversion du numéro public de l'appelé B en un numéro d'appel gardé secret. Ce numéro secret est communiqué au CAS 8 qui établit le demi-appel aval. En outre le PCS 9 ajoute aux informations de signalisation relatives au demi-appel aval une marque qui l'identifie, attestant ainsi auprès de l'usager appelé B que l'appel provient bien du GFU et qu'il fait l'objet d'un contrôle par le PCS 9. Les usagers A et B du GFU peuvent rejeter tous les appels ne provenant pas du PCS 9, c'est-à-dire les appels qui ne sont pas correctement identifiés. Moyennant une telle précaution, il devient alors presque impossible à un fraudeur de court-circuiter le contrôle du GFU.

Le complément de service intitulé "identification d'appels malveillants" peut servir à la journalisation des événements relatifs à la sécurité et notamment à la détection des tentatives d'intrusions frauduleuses dans le GFU. Il peut être également envisager un déclenchement systématique et automatique de l'identification de tout appel intérieur ou extérieur au GFU sécurisé ainsi qu'une autorisation légale d'accès aux informations concernant tous les appels. Il peut être également prévu un stockage de ces informations sur un support physique irréversible afin de pouvoir constituer à plus ou moins longue échéance un service de preuves en cas de contestation d'un appel.

Un système expert peut être chargé de l'exploitation ultérieure de ces informations pour pouvoir produire à chaque usager la liste des appels correspondant à son GFU et même de lui fournir des statistiques et diagrammes synthétiques à partir de règles prédéterminées. Ceci constitue le principe d'un hyper-viseur de sécurité qui peut également être chargé de la facturation du service de l'usager et de recouvrement automatique des sommes dues au titre de l'utilisation du complément de service intitulé "GFU sécurisé".

Une fois la communication établie entre l'appelant A et l'appelé B, le RNIS se comporte alors comme un simple canal de communication entre les deux correspondants A et B. Il est représenté sur la figure 2 par deux lignes parallèles en traits interrompus.

La figure 3 illustre la phase de distribution et de gestion des clés lors de l'établissement d'une communication entre deux usagers.

Le procédé selon l'invention s'articule autour d'un centre de gestion de la sécurité, ou CGS 11, incorporé au PCS 12, commandé par exemple par un serveur de sécurité non représenté.

Cette gestion d'information par le CGS 11 consiste à traiter la signalisation relative à toutes communications sécurisées entre usagers. Pour cela elle effectue l'authentification de l'usager appelant A et de l'usager appelé B ainsi que le contrôle d'accès grâce à sa base de données BD 13 contenant les profils des usagers constituant ainsi un dictionnaire d'usagers. Elle élabore et gère les clés, puis conserve une trace de tous les échanges l'impliquant à des fins de non répudiation. Elle peut également effectuer ensuite une facturation automatique du complément de service offert et

effectuer par exemple la gestion d'un parc de cartes à microcircuit CAM, une carte CAM 14 et 15 étant attribuée personnellement à chaque usager abonné respectivement A et B.

Dans l'élaboration et la gestion des clés, le procédé utilise deux types de clés pour une sécurité efficace.

Un premier type de clés, appelées aussi clés de base CLE, est distribué aux membres du groupe fermé d'usagers abonné GFU au moyen, par exemple, de la carte à microcircuit CAM 14 et 15 attribuée à chacun des usagers abonnés A et B plus une pour le PCS 12. Une clé de base CLE est une clé double comportant une clé secrète KS et une clé publique KP. Cette clé double, ou bi-clé, est utilisée dans des algorithmes cryptographiques de type asymétrique. Chaque usager abonné A et B dispose donc d'une première clé secrète, respectivement KAS et KBS, et d'une deuxième clé publique, respectivement KAP et KBP.

Un deuxième type de clés, appelées clés de trafic KT ou clé de session, est communiqué à l'appelant A et à l'appelé B lors l'établissement de la communication sous la protection par chiffrement au moyen d'un algorithme du type précédent paramétré par les clés de base CLE précitées. Un canal sûr entre le PCS 12 et l'usager est obtenu grâce à la signalisation d'usager à usager SUU en utilisant un procédé de chiffrement par la clé publique KAP de l'usager A assurant ainsi la confidentialité des clés de trafic KT envoyées, suivi d'une signature par la clé secrète KDS du PCS 12 assurant l'authentification de l'origine de l'appel. La transformation réciproque consiste en un déchiffrement au moyen de la clé publique KDP du PCS 12 suivi d'un déchiffrement par la clé secrète de l'usager KAS ou KBS.

La gestion de clés est centralisée à l'intérieur du PCS 12 par le CGS 11. Il peut y avoir une clé de trafic KT par canal pour un accès de base soit un maximum de trois clés pour les canaux 2B plus D.

Le nombre des clés de trafic KT envoyées à un terminal déterminé est fonction du nombre de canaux utilisés. Les mêmes clés sont utilisées pour les deux sens de transmission en "full duplex", ce qui nécessite deux algorithmes de chiffrement paramétrés par la même clé de trafic KT pour chaque canal, dans cet exemple six algorithmes sont alors nécessaires.

Les clés de trafic KT peuvent être les clés secrètes et l'algorithme de chiffrement utilisé peut être un algorithme cryptographique de type symétrique. Une telle gestion de clés nécessite au sein du GFU que la signalisation d'usager à usager SUU correspondant à la demande d'établissement d'une connexion physique ou virtuelle, transite par le PCS 12 où elle est interceptée. Comme évoqué précédemment dans le GFU, il s'agit, au moyen d'un préfixe reconnu par le commutateur d'accès au service CAS 16, d'acheminer la signalisation d'usager à usager SUU vers le PCS 12 apte à traiter le complément de service GFU. C'est à ce niveau que se fait le contrôle d'accès initial au vu du numéro de l'appelant A, la recherche du numéro traduit de l'appelé B, la commande de l'établissement du demi-appel aval par le CAS 16, et l'authentification des correspondants.

Après vérification de compatibilité de GFU, le PCS 12 transmet à l'appelant A et à l'appelé B leur clé de trafic KT respective. Chaque lot de clés de trafic KT est rassemblé dans un champ mini-message, chiffré en une seule fois, de la signalisation d'usager à usager SUU. Un champ mini-message permet aux usagers d'échanger des champs d'informations de 32 octets lors de l'établissement ou de la libération de la communication ou en dehors de toute communication. Partant du principe selon lequel un accès à la base de données BD 13 liée au PCS 12 est nécessaire pour connaître le GFU d'appartenance des deux correspondants A et B ainsi que le numéro traduit de l'appelé B, il apparaît naturel que leur clé publique KAP et KBP s'y trouvent également sous la forme d'attributs supplémentaires.

Suivant la norme CCITT n° 7, 17, l'espace prévu pour véhiculer les clés de chiffrement comporte 32 octets soit 256 bits pouvant être porté à 128 octets et il est également prévu deux types de signalisation reposant sur le sous système de transfert de message SSTM. Une signalisation liée à une demande d'établissement de connexion porte une étiquette la rattachant à cette communication. Il existe également une possibilité d'utiliser une signalisation d'usager à usager SUU en dehors de toute requête de connexion. L'espace réservé pour le mini-message étant suffisant dans le cas d'un chiffrement par un algorithme cryptographique de type symétrique utilisant une clé de 64 bits, la capacité de transport de quatre clés suffit pour l'accès de base n' utilisant que trois clés. Dans le cas contraire, une suite de

mini-messages véhiculés par la signalisation usager à usager SUU apportera la capacité de transport du nombre de clés nécessaire.

Considérant l'accès à la base de données BD 13 cité précédemment, un double chiffrement est appliqué sur l'ensemble du champ mini-messages, correspondant à un bloc de 256 bits, sur lequel sont appliquées ensuite successivement deux transformations selon un algorithme cryptographique asymétrique. Une fois la communication établie entre les deux abonnés, le chiffrement de la communication par un algorithme cryptographique symétrique est réalisé au niveau trois du modèle OSI par une sous couche de sécurité ISTCS abréviation anglo-saxonne pour "Integrated Services Trusted Communication Sublayer", ceci assurant la confidentialité et l'intégrité des informations échangées via le RNIS.

Une raison essentielle pour le choix d'un procédé de chiffrement utilisant un algorithme cryptographique symétrique et réalisé au niveau 3 par la sous-couche ISTCS, est que l'accès ultérieur aux canaux B et D en mode paquet doit pouvoir se faire de façon transparente vis-à-vis du chiffrement. Le routage des paquets s'effectue par le niveau 3, une contrainte importante étant de respecter la nécessité de transparence du chiffrement par rapport aux services support transitant également via les couches 1 à 3 du modèle OSI.

Le contrôle d'accès introduit précédemment s'assure du droit d'un usager abonné d'accéder au service qu'il demande. Ce contrôle est basé sur un procédé d'authentification préalable réalisé à partir d'un ordinateur frontal de sécurité interposé entre l'usager et le réseau et dénommé ci-après frontal de sécurité

Considérant que les services d'authentification, de contrôle d'accès et de non répudiation sont intrinsèquement liés, le procédé selon l'invention propose un mécanisme de double authentification présentant l'avantage de cumuler le traitement de ces trois services.

Une solution simple pour permettre la mise en oeuvre de ce mécanisme consiste à utiliser un mot de passe que l'usager doit entrer par l'intermédiaire du clavier du frontal de sécurité. Néanmoins la sécurité peut être largement accrue à peu de frais en exploitant les principes concernant la gestion de clés mentionnée plus haut.

En effet, l'inconvénient majeur du mot de passe est qu'il transite en clair sur le réseau étant ainsi sensible à une attaque par interception et rejeu. Des développements plus ou moins complexes sur des systèmes à apports nuls de connaissances, parmi lesquels le schéma de Lamport, permettent un renouvellement du mot de passe à chaque utilisation.

Le procédé selon l'invention exploite le fait que le contrôle d'accès physique a déjà été effectué par le PCS 12 qui a contrôlé l'appartenance de l'appelant et de l'appelé usagers abonnés au même GFU. Le PCS 12 a ensuite fait parvenir à chacun des correspondants leurs clés de trafic KT communes. Celle-ci sont stockées dans le frontal de sécurité qui opère le chiffrement pour la durée de la communication. La transmission d'une, deux ou trois clés de trafic KT en fonction du service, via la signalisation d'usager à usager SUU dans le champ mini-messages issu du PCS 12, est intercepté par le frontal de sécurité qui produit une requête d'authentification. Celle-ci se traduit alors par une demande de mot de passe auprès de l'usager abonné. Il est rappelé que la notion d'usager abonné recouvre aussi bien une personne physique qu'une application qui doit être adaptée à ce mode de fonctionnement et au sein de laquelle le mot de passe d'accès au réseau devra être caché. Par exemple, un blocage avec interdiction d'accès au RNIS dès que l'application est interrompue peut être envisagé. Une fois le mot de passe entré par l'usager abonné, celui-ci est chiffré par la première clé de trafic KT courante. Le frontal de sécurité qui opère le chiffrement doit donc être accessible aussi bien par le plan usager qui fournit les services réseaux que par le plan de signalisation où va transiter le mot de passe chiffré.

Une autre solution consiste à utiliser une carte à micro-circuit CAM contenant des éléments secrets tels que mot de passe, clé secrète du terminal et clé publique du PCS, et un lecteur de cartes à micro-circuit CAM couplé au frontal de sécurité.

De cette façon l'interface devient inutilisable en mode chiffré dès lors que la carte à micro-circuit CAM aura été retirée et stockée dans un coffre fort par exemple.

Il est à remarquer que le mot de passe n'est pas en principe chiffré deux fois de la même manière dans le mesure où la ou les clés de trafic KT sont changées à chaque communication.

Cependant il est bien évident que le PCS disposera d'un stock limité de clés de trafic KT qu'il distribuera à tour de rôle aux usagers abonnés du GFU en instance de communication.

Il est donc nécessaire de prévoir un système de génération et un stock de clés dont le nombre et la durée de vie seront dimensionnés en fonction du nombre d'usagers abonnés et du nombre de moyen de communication par usager abonné et par unité de temps. Un compromis entre la capacité à produire des clés aléatoires possédant de bonne qualité cryptographique et de plus ou moins renouveler les clés du trafic KT est donc à déterminer. Un nombre trop élevé de réutilisations d'une même clé de trafic KT est à éviter dans la mesure ou ceci accroît le risque de compromission.

Cependant, il se peut qu'un fraudeur puisse réussir à constituer un dictionnaire des clés de trafic KT utilisées par le PCS pour réussir à s'interposer. Ceci est toutefois rendu difficile du fait de la confidentialité et de l'intégrité du transfert de clés de trafic KT entre le PCS et le frontal de sécurité de l'usager abonné grâce notamment au double chiffrement utilisant l'algorithme cryptographique asymétrique.

De même, de façon symétrique le protocole d'authentification peut s'appliquer à l'usager abonné appelé via son frontal de sécurité respectif. Le PCS lui envoie sa ou ses clés de trafic KT avec vérification de compatibilité du GFU sécurisé. La ou les clés sont envoyées dans le champ mini-messages de la signalisation d'usager à usager SUU en demandant l'établissement d'une communication, dans ce cas, demi-appel aval.

Le PCS bloque le circuit physique tant que les deux correspondants ne sont pas correctement authentifiés. Pour se faire, il est fait appel à la capacité du PCS de gérer deux demi-appels distincts : un demi-appel amont avec l'appelant , et un demi-appel aval avec l'appelé. Dans le cas favorable le PCS envoie, au CAS qui a reconnu l'appel comme requérant le complément de service GFU, la demande d'établissement de la communication entre les deux usagers abonnés. Le contrôle d'accès peut être amélioré en ajoutant à la fonction des mots de passe du PCS une fonction de lecture des restrictions d'accès propres à chaque usager abonné à l'intérieur de la base de données BD accessible par le PCS. Outre le numéro du groupe fermé d'usagers abonnés GFU et la clé publique de

l'usager abonné, des informations relatives au profil de chaque usager abonné doivent être accessibles en lecture.

Une fonction supplémentaire de signalisation d'événements peut être additionnée au mécanisme d'accès sécurisé qui vient d'être décrit.

Diverses causes de non avertissement d'un appel peuvent être signalées aux usagers. Les messages correspondant sont envoyés par le CAS sur ordre du PCS pour informer l'appelant et l'appelé de la cause du refus de l'appel. Différentes natures de causes de refus peuvent se présenter :

- un appelant et un appelé appartiennent à des GFU différents, il faut alors avertir l'appelant,

- un défaut d'authentification de l'appelant, celui-ci doit en être averti,

- un défaut d'authentification de l'appelé, il faut en avertir les deux correspondants par des messages différents,

- une surcharge du réseau ou du PCS, il faut en avertir l'appelant qui devra rappeler ultérieurement.

Un scénario d'échange de signalisation d'usager à usager SUU conduisant à une communication sécurisée via RNIS est détaillé ci-dessous :

Un usager A demande une communication sécurisée avec un usager B via la signalisation d'usager à usager SUU. Le CAS reconnaît le complément de service GFU sécurisé et aiguille la signalisation d'usager à usager SUU vers le PCS. Le PCS interroge sa base de données BD sur les deux correspondants A et B en vérifiant dans le GFU concerné si le numéro d'appel de B correspond bien à ce groupe fermé d'usagers abonnés en vérifiant si les clés publiques et les mots de passe ainsi que les restrictions d'accès sont conformes, ensuite le PCS distribue à l'usager abonné A une clé de trafic et l'usager abonné A doit s'authentifier, cette authentification est envoyée au PCS qui vérifie l'identité de l'usager abonné A par l'intermédiaire de sa base de données BD. Le PCS transmet à l'usager abonné B une clé de trafic et doit également s'authentifier, le PCS reçoit cette authentification et vérifie l'identité de l'usager abonné B. Si tout est exact le PCS demande au CAS d'établir la communication et la connexion est ensuite établie entre les deux usagers abonnés A et B.

Le scénario décrit ci-dessus représente le cas d'un déroulement favorable. Il est toutefois nécessaire de prévoir un mécanisme de reprise en cas d'erreur de l'opérateur sur l'entrée de son mot de passe, par exemple trois tentatives autorisées, sauf si tous les frontaux de sécurité sont équipés d'un lecteur de cartes à micro-circuit CAM.

Un premier mode de réalisation d'un dispositif pour la mise en oeuvre du procédé selon l'invention est illustré par la figure 4.

Sur cette figure un RNIS 18 du type représenté à la figure 2 est utilisé pour la transmission d'une communication sécurisée entre deux usagers abonnés A et B, un usager abonné appelant A à gauche et un usager abonné appelé B à droite du RNIS 18. Chaque usager abonné A et B dispose d'un terminal 19, 20 couplé à un frontal de sécurité 21, 22 qui donne accès à un autocommutateur 23, 24 connu sous l'abréviation anglo-saxonne PABX, "Private Automatic Branch Exchange", connecté directement au RNIS 18. Le frontal de sécurité 21, 22 est couplé respectivement au terminal 19, 20 de l'usager A et B et au PABX 23, 24 par une interface à débit de base, aussi appelée interface S de terminal. L'interface S_0 étant réservé pour les terminaux intelligents du type micro-ordinateur suivant la dénomination de la norme ECMA abréviation anglo-saxonne pour "European Computer Manufacturer Association". Un même PABX 23, 24 peut recevoir sur son entrée plusieurs accès d'usager. Il a dans ce cas un rôle fédérateur. Sa sortie est couplée au RNIS 18 par l'intermédiaire d'une interface T_0 ou T_2, également soumise à la norme ECMA. Un lecteur de cartes 25, 26 à micro-circuit, ou carte à puces, est connecté au frontal de sécurité. Le lecteur reçoit une carte à micro-circuit 27, 28 appartenant respectivement à l'usager abonné A et B. Cette carte 27. 28 contient les éléments secrets tels que mot de passe, clé secrète du terminal et clé publique du PCS. L'interface entre l'usager et le RNIS devient inutilisable en mode chiffré dès lors que la carte à micro-circuit CAM est retirée du lecteur de cartes à micro-circuit CAM. Chaque carte à micro-circuit CAM porte un numéro d'identification inscrit dans la puce lors de sa fabrication et qui est lu par le lecteur de cartes à micro-circuit CAM à chaque utilisation en mode chiffré de l'un des terminaux raccordés au frontal de sécurité. Lors de la première utilisation d'un terminal ou à l'occasion d'un renouvellement des éléments secrets contenus dans la carte à micro-circuit CAM, l'opérateur ou l'usager abonné commande la

validation de la carte à micro-circuit CAM introduite dans le lecteur par l'intermédiaire du terminal. A chaque nouvelle utilisation le lecteur de cartes à micro-circuit CAM n'accepte de lire les éléments secrets contenus dans la puce que si le numéro d'identification de la carte à micro-circuit CAM correspond au dernier numéro validé. Le fonctionnement du frontal de sécurité est décrit en détail ci-après :

Le frontal de sécurité réalise un chiffrement/déchiffrement sur la base d'un algorithme cryptographique symétrique implémenté au niveau de la couche 3 du modèle OSI pour les communications via les canaux B et D. En outre le chiffrement/déchiffrement est accessible par un identificateur de point d'accès service connu sous l'abréviation anglo-saxonne SAPI pour "Service Access Point Identifier" réservé à la signalisation d'usager à usager SUU pour sécuriser les échanges de signalisation.

Il réalise également un chiffrement/déchiffrement selon l'algorithme cryptographique asymétrique où le SAPI est réservé à la signalisation d'usager à usager SUU, sur le champ de mini-message de 32 à 128 octets. Ceci a pour but d'acquérir la ou les clés de trafic KT envoyées par le PCS dans le champ mini-message. Cette opération nécessite le double déchiffrement précédant, la troncature du mini-message en clé de trafic KT puis la mise à la clé des algorithmes cryptographiques symétriques de chiffrement/déchiffrement du circuit de données.

A la réception d'un message de signalisation d'usager à usager SUU portant la marque du complément de service GFU sécurisé apposée par le PCS, le frontal de sécurité produit une demande de mots de passe vers l'usager abonné, ou le lecteur de carte à micro-circuit CAM, qui doit fournir en échange le mot de passe inscrit sur celle-ci. En réponse à cette requête le frontal de sécurité envoie le mot de passe chiffré avec la première clé de trafic KT courante en direction du PCS. L'acheminement du message de signalisation est assuré par le CAS. Le frontal de sécurité se met alors en attente de signalisation issue du CAS. Deux éventualités peuvent alors se présenter :

- en cas d'erreur sur l'entrée du mot de passe, le CAS reémet une demande d'authentification, le processus peut être renouvelé une fois,

- en cas d'authentification correcte des deux correspondants par le PCS, le frontal de sécurité reçoit du CAS un message confirmant le traitement de l'appel.

Dans le cas favorable, la communication se poursuit selon la procédure habituelle et le frontal de sécurité démarre le chiffrement sur interception du message de signalisation de connexion échangé entre l'appelé et l'appelant.

La figure 5 représente le mode de réalisation de la figure 4 sous la forme d'une structure en couches suivant le modèle OSI.

Cette représentation est symétrique par rapport à un RNIS du type décrit précédemment dans les figures précédentes.

Le terminal de l'usager abonné 30A, 30B est représenté par sept couches de niveau respectif 7 à 1, la couche supérieure correspondant au niveau 7. Le frontal de sécurité 31A, 31B est représenté par trois couches de niveau respectif 3 à 1, surmontées de la sous-couche de sécurité ISTCS de niveau 3. Le chiffrement est réalisé à ce niveau. L'interface S_0 correspond à la couche de niveau 1, ou niveau physique.

Le PABX 32A, 32B est représenté sous la forme de trois couches de niveau respectif 3 à 1, appelé également TNA, abréviation de Terminaison Numérique d'Abonnés, et une dernière couche de niveau A représente un TNR, 33A, 33B abréviation de Terminaison Numérique de Réseau.

Un support physique de transmission 34, représenté sur la figure 5 par une couche hachurée, permet de relier les couches de niveau inférieur 1 respectives au terminal 30A, 30B au frontal de sécurité 31A, 31B, au TNA 32A, 32B et au TNR 33A, 33B jusqu'au RNIS 29. La zone de communication sécurisée est représentée sur la figure 5 à l'intérieur d'une ligne fermée discontinue.

Un deuxième mode de réalisation d'un dispositif pour la mise en oeuvre du procédé selon l'invention est illustré par la figure 6.

Dans ce mode de réalisation, une première installation terminale d'usager abonnés appelant ITU A comporte une grappe de terminaux 35i dont le nombre maximal ne peut excéder huit. Les terminaux 35i sont connectés entre eux par un bus passif 36 relié lui-même à un frontal de sécurité 37 par l'intermédiaire d'une interface S_0, et adressables

séparément grâce au protocole LAPD, abréviation anglo-saxonne pour "Link Access Protocol on the D Channel" permettant des échanges sécurisés entre les différents équipements assurant les fonctions de la couche 2 du modèle OSI, et au sous-adressage. La sortie du frontal de sécurité 37 est couplée à l'entrée d'un RNIS 38 également par une interface S_0. Comme pour le premier mode de réalisation de la figure 4, l'accès de l'usager au frontal de sécurité 37 se fait au moyen d'un lecteur 39 de carte à micro-circuit CAM 40. Une deuxième installation terminale d'usagers abonnés appelés, ITU B, connectée en sortie du RNIS comporte un PABX 41 connecté au RNIS 38 par l'intermédiaire d'une interface T_0 ou T_2. Les N sorties du PABX 41 sont respectivement couplées par l'intermédiaire d'une interface S_0 à une grappe de terminaux via un frontal de sécurité 43 dont l'installation est identique à celle de l'ITU A comportant un lecteur 44 de carte à micro-circuit CAM 45.

L'interface S_0 commune à la grappe de terminaux 35i, 42i est sécurisée.

Le frontal de sécurité 37, 43 gère respectivement l'adresse origine et destinataire mais ne gère pas la sous-adresse origine et destinataire relative à un terminal appelé au sein de ITU B et un terminal appelant au sein de ITU A. Il ne distingue pas les terminaux 35i, 42i connectés à l'interface S_0.

Le sous-adressage, qui est une méthode connue en RNIS, exclut naturellement l'interfonctionnement avec des terminaux non RNIS qui sont incapables de générer une sous-adresse. L'adresse origine, identifiant l'interface S_0 et le frontal de sécurité 37, 43, est associée à une sous-adresse d'origine qui identifie le terminal destinataire au sein de la grappe de terminaux 42_i. Le PABX 41 permet de mettre en communication via le RNIS 38, le terminal de l'usager abonné appelant A avec le terminal de l'usager abonné appelé B dont les sous-adresses respectives correspondent. L'usager abonné appelant A a donc la possibilité de sélectionner une entité déterminée à l'intérieur de l'installation terminale ITU de l'usager abonné appelé B en complétant, par exemple, l'adresse principale par 1 à 4 chiffres supplémentaires définissant une sous-adresse. Cette information supplémentaire est transportée de façon transparente par le réseau 38.

Une extension possible de l'invention concerne la sécurisation de l'interface S_2, ainsi que tout autre type d'accès quelque soient le nombre de canaux, le type de canaux et leur débit.

Enfin, l'objet de l'invention qui s'intéresse essentiellement aux communications entre installations fixes peut également être étendu aux communications entre les mobiles dans le cadre du GSM, abréviation pour Groupe Spécial Mobiles.

Le but d'un réseau GSM est d'offrir des services de télécommunications à des abonnés quels que soient leurs déplacements à l'intérieur d'une zone de service, définie par un opérateur ou même plusieurs opérateurs ayant passé des accords mutuels. Pour ce faire l'abonné mobile utilise une station mobile dont l'originalité est d'être constituée de deux éléments séparables :

- un équipement mobile qui fournit les capacités de radiocommunications et logicielles nécessaires au dialogue avec le réseau, et

- une carte amovible, du type carte à micro-circuit CAM qui contient les caractéristiques de l'abonné et de ses droits, en particulier son identité internationale.

REVENDICATIONS

1. Procédé de sécurisation d'un réseau numérique à intégration de services, ou RNIS, du type mettant en oeuvre un ensemble de téléservices offerts aux usagers du réseau, avec des options appelées compléments de service, caractérisé en ce qu'il consiste pour définir un nouveau complément de service intitulé groupe fermé d'usagers sécurisé (1_1 à 1_i) accessible aux usagers par abonnement, dans l'environnement d'un point de commande des services (2 ; 9 ;12) du RNIS (3), à reconnaître par un commutateur d'accès au service (8 ; 16) du RNIS, le complément de service groupe fermé d'usagers sécurisé, à aiguiller la signalisation d'usager à usager vers le point de commande des services (2 ; 9 ; 12) du RNIS, à authentifier les correspondants en instance de communication et à contrôler les droits d'accès des correspondants par une lecture d'une base de données (10 ; 13) contenant la liste des abonnés au complément de service groupement fermé d'usagers sécurisé, pour permettre d'établir au moins une communication sécurisée entre au moins deux correspondants abonnés d'un même service, quel que soit le service, la sécurisation étant transparente vis-à-vis de chacun des correspondants pour le service demandé.

2. Procédé selon la revendication 1, caractérisé en ce que l'authentification consiste d'une part, à attribuer à chaque correspondant ainsi qu'au point de commande des services (2 ; 9 ; 12), une clé de base (CLE) comportant une clé secrète (KS) et une clé publique (KP), et d'autre part, lors de l'établissement de la communication, à envoyer à chaque correspondant, via la signalisation usager à usager du RNIS, au moins une clé de trafic (KT) distribuée par le point de commande des services (2 ; 9 ; 12), la confidentialité des échanges des clés de trafic (KT) étant assurée par un premier chiffrement de la clé de trafic (KT) par la clé publique de chaque correspondant (KAP et KBP) suivi d'une deuxième chiffrement par la clé secrète (KS) du point de commande des services (2 ; 9 ; 12).

3. Procédé selon l'une quelconque des revendications 1 à 2, caractérisé en ce qu'il consiste en outre, à mémoriser tous les échanges entre correspondants sur un support physique.

4. Dispositif pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comporte d'une

part, un frontal de sécurité (21 ; 31A ; 37) disposé en coupure entre au moins un terminal (19 ; 30A ; 35i) d'au moins un correspondant appelant (A) et le RNIS, et un frontal de sécurité (22 ; 31B ; 43i) disposé en coupure entre au moins un terminal (20 ; 30B ; 42i) d'au moins un correspondant appelé (B) et le RNIS, les deux frontaux de sécurité assurant un chiffrement ou déchiffrement des informations contenues dans la communication transitant via le RNIS, et comporte d'autre part, un serveur de sécurité (11) couplé au point de commande des services (2 ; 9 ; 12) permettant la gestion de la sécurité des informations.

5. Dispositif selon la revendication 4, caractérisé en ce qu'un lecteur de carte à micro-circuit (25 ; 26 ; 39 ; 44) est couplé à chaque frontal de sécurité permettant la lecture d'une carte à micro-circuit (27 ; 28 ; 40 ; 45) contenant la clé publique (KP) du point de commande des services (2 ; 9 ; 12) et la clé secrète (KS) de l'abonné au complément de service groupe fermé d'usagers sécurisé.

6. Dispositif selon l'une quelconque des revendications 4 et 5, caractérisé en ce qu'il comporte en outre, au moins un autocommutateur (41) inséré entre au moins un frontal de sécurité (43_i) et le RNIS (38).

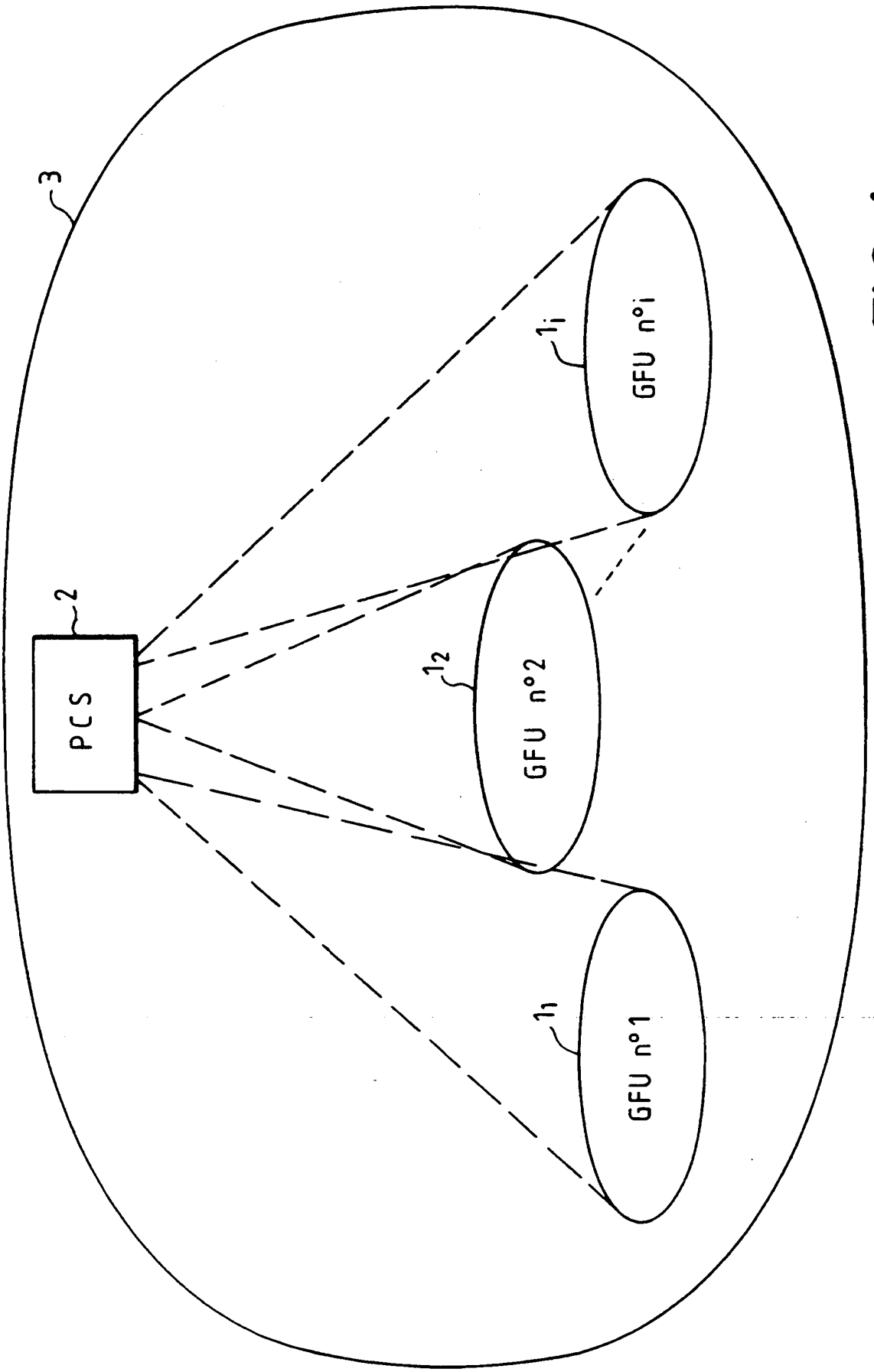


FIG. 1

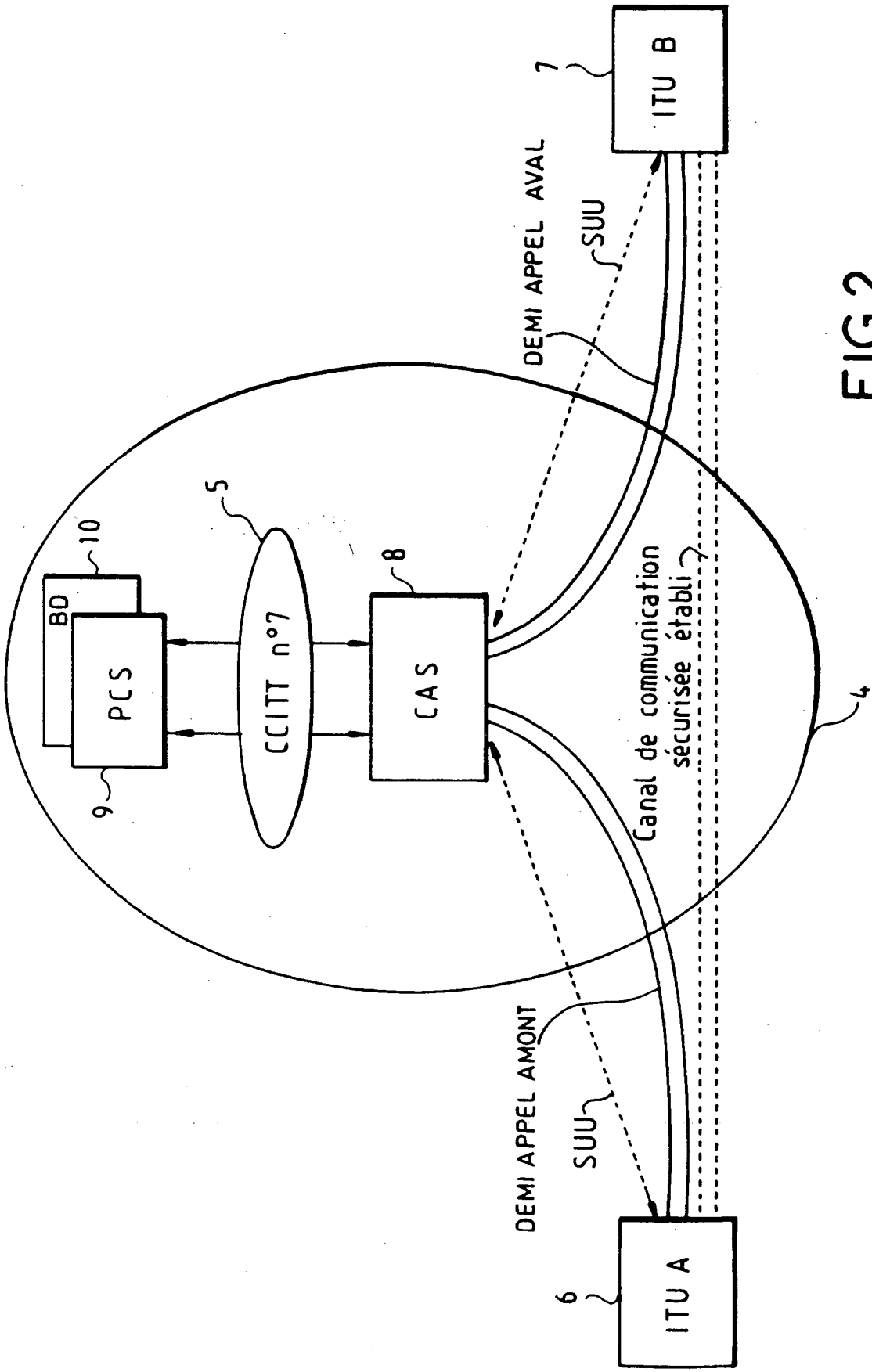


FIG.2

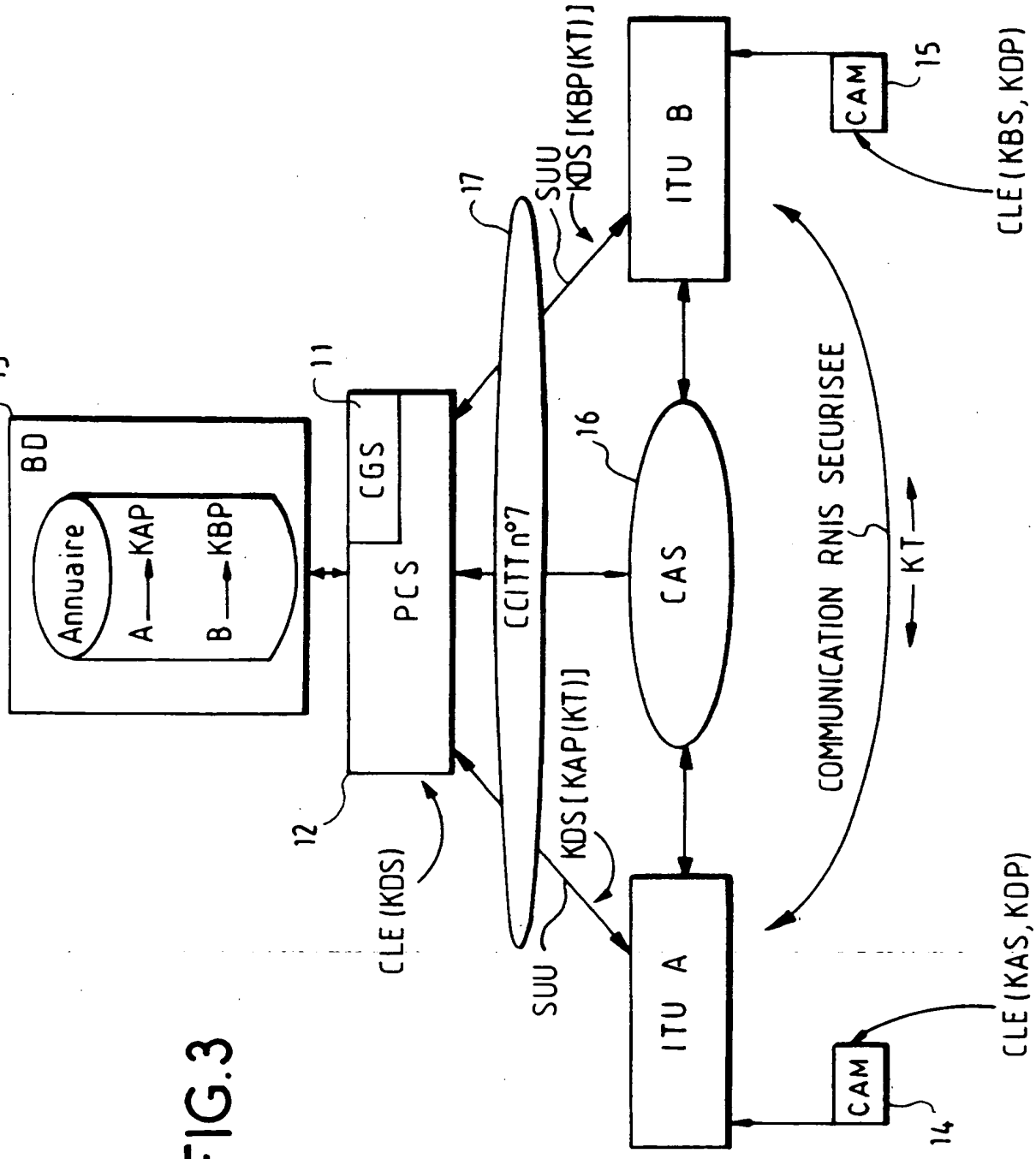


FIG.3

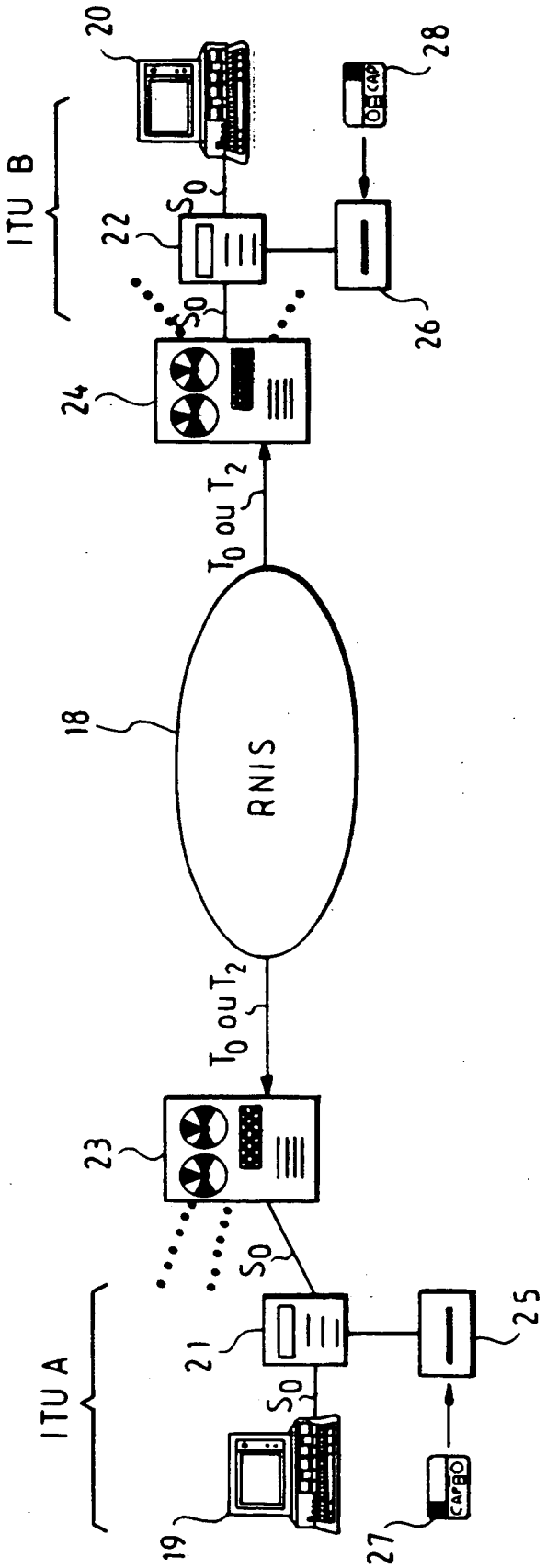


FIG.4

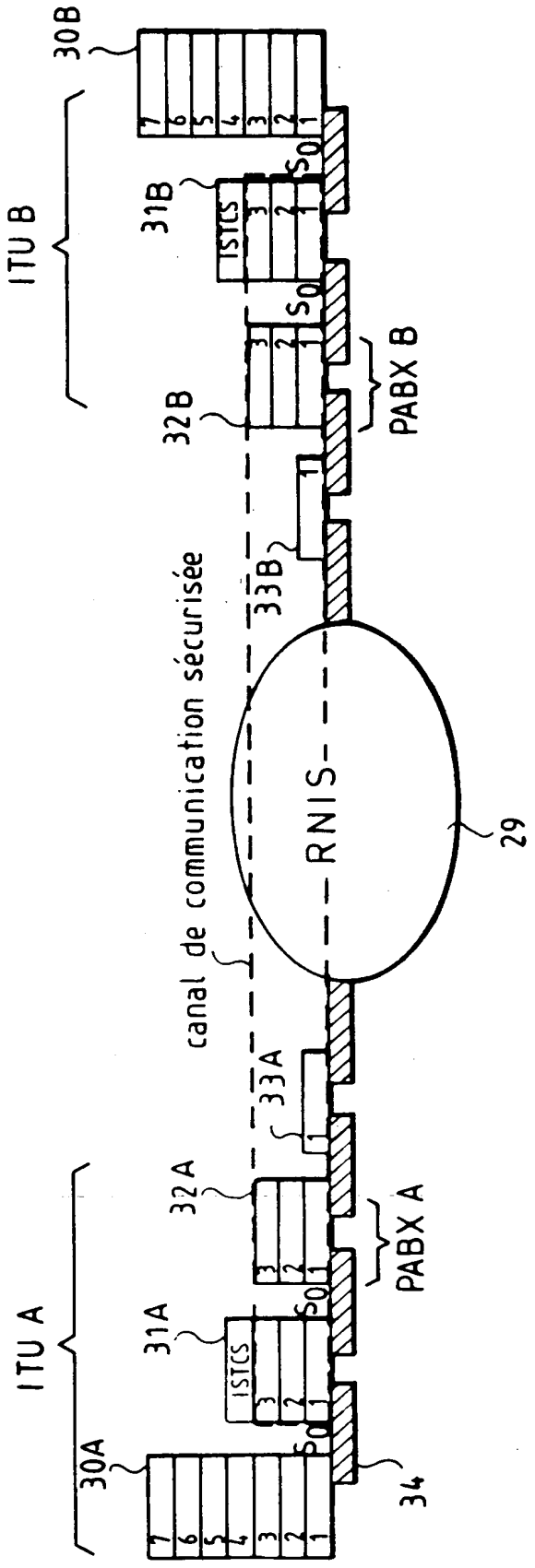


FIG.5

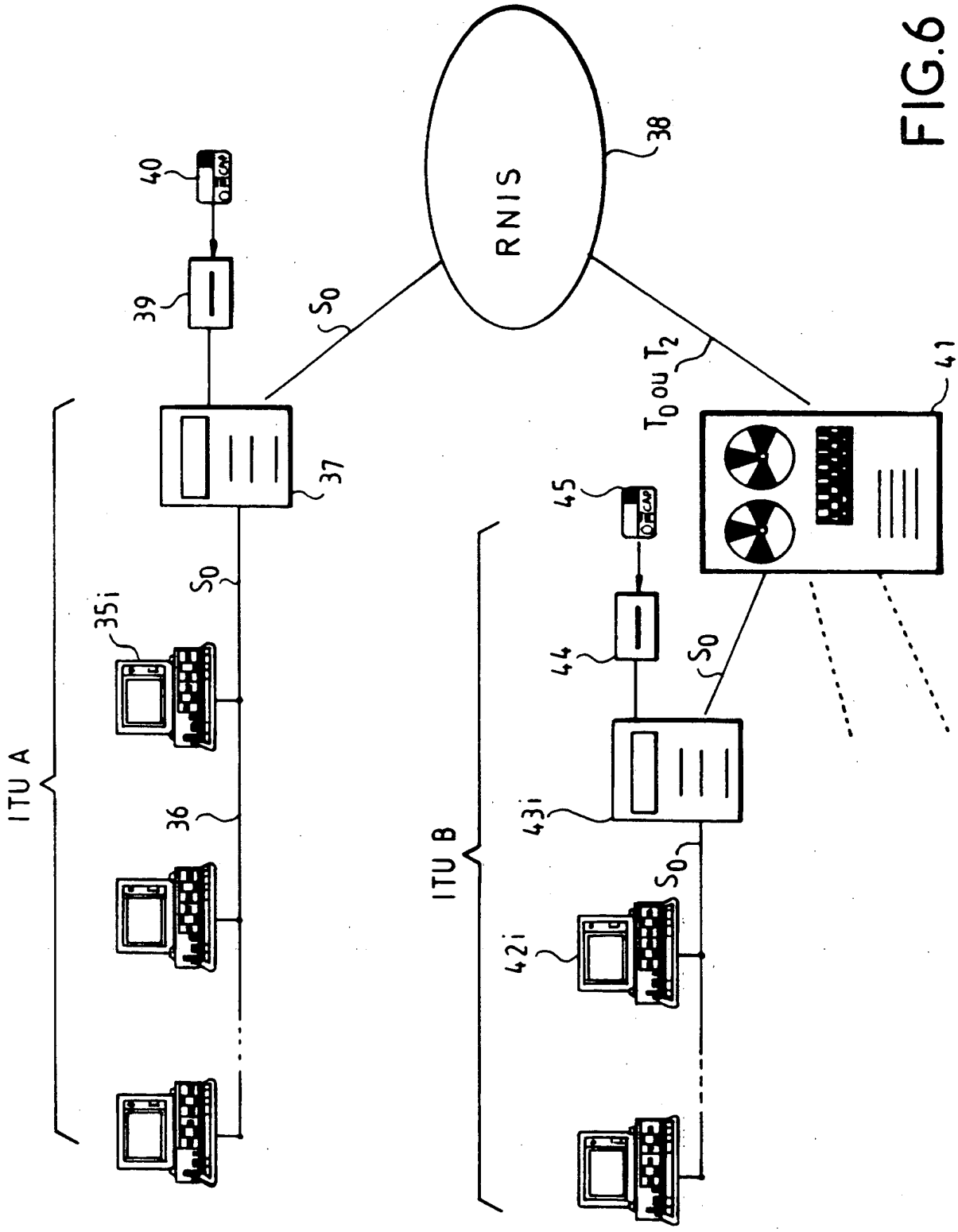


FIG.6

REPUBLIQUE FRANÇAISE

2709903

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 493793
FR 9310781

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	PROCEEDINGS OF SOUTHERN AFRICAN CONFERENCE ON COMMUNICATIONS AND SIGNAL PROCESSING COMSIG 88 24 June 1988, Pretoria (SA) NEW YORK (US) pages 165-170, G.J. CLAASSEN & G.J KÜHN "SECURE COMMUNICATION PROCEDURE FOR ISDN" * page 167, colonne de gauche, ligne 23 - colonne de droite, ligne 1 * * page 169, colonne de gauche, ligne 1 - page 170, colonne de droite, ligne 27 * * figure 7 * ---	1,2,4
A	ELECTRICAL COMMUNICATION, vol.60, no.1, BRUSSELS BE pages 63 - 70 K.PRESTTUN 'SECURITY MEASURES IN COMMUNICATION NETWORKS' * page 66, colonne de gauche, ligne 48 - page 68, colonne de gauche, ligne 25 * * figure 4 * ---	1,2,4
A	BULLETIN DE LASSOCIATION SUISSE DES ELECTRICIENS, vol.77, no.1, 11 Janvier 1986, SWITZERLAND pages 5 - 11 K. SIUDA 'TECHNISCHE MASSNAHME FÜR DIE SICHERE INFORMATIONSÜBERTRAGUNG IN ZUKÜNFTIGEN FERNEMELDENETZEN (ISDN)' * page 8, colonne du milieu, ligne 27 - colonne de droite, ligne 63 * * page 9, colonne de droite, ligne 1 - page 11, colonne du milieu, ligne 26 * * figures 3,4 * ---	1,2,4

-/--

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

H04L
H04M

1

Date d'achèvement de la recherche	Examinateur
30 Mai 1994	Lydon, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2709903

N° d'enregistrement national

FA 493793
FR 9310781

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	TELCOM REPORT, vol.16, no.2, 1 Mars 1993, MUNCHEN DE pages 96 - 99 H. BLAB 'SICHER IST SICHER' * page 99, colonne de gauche, ligne 30 - colonne du milieu, ligne 36 * * figure 4 *	4
A	PATENT ABSTRACTS OF JAPAN vol. 12, no. 124 (E-601) 16 Avril 1988 & JP-A-62 249 548 (FUJITSU) 30 Octobre 1987 * abrégé *	1,4

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

Date d'achèvement de la recherche	Examinateur
30 Mai 1994	Lydon, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)